

EXPRESS MAIL NO.: EV 353464794 US

DATE OF DEPOSIT: July 3, 2003

This paper and fee are being deposited with the U.S. Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

NISHI PASARUA

Name of person mailing paper and fee

[Signature]

Signature of person mailing paper and fee


ENCRYPTED RESPONSE SMART BATTERY

Inventors: Larry G. Edington
12708 Red Deer Pass
Austin, TX 78729

James E. Dailey
2305 Falkirk Cove
Round Rock, TX 78681

Assignee: Dell Products L.P.
One Dell Way
Round Rock, Texas 78682

David L. McCombs
HAYNES AND BOONE, L.L.P.
901 Main Street
Suite 3100
Dallas, Texas 75202-3789
(214) 651-5533

EXPRESS MAIL NO.: <u>EV 353464794 US</u> DATE OF DEPOSIT: <u>July 3, 2003</u>	
This paper and fee are being deposited with the U.S. Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450	
<u>Nishi PASARUA</u> Name of person mailing paper and fee	 Signature of person mailing paper and fee

ENCRYPTED RESPONSE SMART BATTERY

5

Background

The present disclosure relates generally to information handling systems, and more particularly to techniques for authenticating rechargeable smart batteries commonly used to provide power to portable information handling system components such as notebook computers, personal digital assistants, cellular phones and gaming consoles.

As the value and use of information continues to increase, individuals and businesses seek additional ways to process and store information. One option available to users is information handling systems. An information handling system generally processes, compiles, stores, and/or communicates information or data for business, personal, or other purposes thereby allowing users to take advantage of the value of the information. Because technology and information handling needs and requirements vary between different users or applications, information handling systems may also vary regarding what information is handled, how the information is handled, how much information is processed, stored, or communicated, and how quickly and efficiently the information may be processed, stored, or communicated. The variations in information handling systems allow for information handling systems to be general or configured for a specific user or specific use such as financial transaction processing, airline reservations, enterprise data storage, or

global communications. In addition, information handling systems may include a variety of hardware and software components that may be configured to process, store, and communicate information and may include one or more computer systems, data storage systems, and networking systems.

5

A battery converts chemical energy within its material constituents into electrical energy in the process of discharging. A rechargeable battery is generally returned to its original charged state (or substantially close to it) by passing an electrical current in the opposite direction to that of the discharge. Presently well known rechargeable battery technologies include Lithium Ion (LiON), Nickel Cadmium (NiCd), and Nickel Metal Hydride (NiMH). In the past, the rechargeable batteries (also known as "dumb" batteries) provided an unpredictable source of power for the portable devices, since typically, a user of the device powered by the battery had no reliable advance warning that the energy supplied by the rechargeable battery was about to run out.

15

Today, through the development of "smart" or "intelligent" battery packs, batteries have become a more reliable source of power by providing information to a device of the information handling system and eventually to a user as to the state of charge, as well as a wealth of other information. The smart rechargeable battery, which is well known, is typically equipped with electronic circuitry to monitor and control the operation of the battery. The information is typically communicated using a well-known System Management Bus (SMBus), which is widely used in the industry. Information pertaining to the smart battery and being communicated via the SMBus connection may include data elements such as smart battery status, manufacturer name, serial and model number, voltage, temperature and charge status.

20

25

Smart batteries, which may be original equipment manufactured (OEM) or in-house manufactured, typically undergo extensive testing and validation procedures before they are approved and qualified to be included in a portable information handling system device by the manufacturer of the portable device. The portable device powered by the smart battery may also undergo additional testing prior to being shipped to a customer. The high cost of many smart batteries has attracted an increasing number of counterfeit smart battery vendors to (re)manufacture and sell genuine-like smart batteries at lower prices to unsuspecting customers. The counterfeit batteries are typically able to emulate virtually any genuine smart battery by emulating their manufacturer, model name, and serial number. An authentication process to identify the genuine smart batteries is almost non-existent. These counterfeit batteries, which often go through very minimal testing and validation procedures, may pose as a serious hazard to the unsuspecting customers. For example, if the counterfeit smart battery does not properly safeguard the charging process then excessive heating caused during the charging process may cause an explosion. This may result in a significant liability problem for the manufacturers of the information handling system device and/or the OEM smart battery.

Therefore a need exists to properly safeguard the charging process of a smart battery. More specifically, a need exists to develop tools and techniques for disabling the charging process for counterfeit smart batteries. Accordingly, it would be desirable to provide tools and techniques for charging authenticated smart batteries included in an information handling system absent the disadvantages found in the prior methods discussed above.

Summary

The foregoing need is addressed by the teachings of the present disclosure, which relates to a system and method for authenticating a smart battery to ensure a safe charging process. According to one embodiment, in a method and system for authenticating a smart battery for charging, the smart battery receives an encrypted random string. The smart battery is operable to provide power to an information handling system device. In this embodiment, the device performs the encryption function and the smart battery performs the decryption function. A controller of the device generates the encrypted random string by generating a random string and encrypting the random string with an encryption key. The smart battery decrypts the encrypted random string with the encryption key to recover the random string and transfer the random string to the device. The device verifies that the random string is unchanged to authenticate the smart battery for the charging. If the random string has been modified then the smart battery is disabled from the charging.

In one embodiment, the encryption/decryption function is performed by the device and the smart battery. In this embodiment, the smart battery encrypts the recovered random string with another encryption key. The encrypted random string is transferred to the device. The device decrypts the encrypted random string with the another encryption key to recover the random string. The device verifies that the random string is unchanged to authenticate the smart battery for the charging. If the random string has been modified then the smart battery is disabled from the charging. The use of two encryption keys advantageously provides additional security in the authentication process.

Several advantages are achieved by the method and system according to the illustrative embodiments presented herein. The embodiments advantageously

provide for a reduced occurrence of operating conflicts and improved reliability while reducing the number of components.

Brief Description of the Drawings

5

FIG. 1 illustrates a diagrammatic representation of a smart battery authentication system for authenticating a smart battery, according to an embodiment;

10

FIG. 2 illustrates a diagrammatic representation of the smart battery system of FIG. 1 having a processor and smart electronics, according to an embodiment;

FIG. 3 is a flow chart illustrating a method for authenticating the smart battery, according to an embodiment; and

15

FIG. 4 illustrates a block diagram of an information handling system to implement method or apparatus aspects of the present disclosure, according to an embodiment.

20

Detailed Description

Novel features believed characteristic of the present disclosure are set forth in the appended claims. The disclosure itself, however, as well as a preferred mode of use, various objectives and advantages thereof, will best be understood by
25 reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings. The functionality of various devices or components described herein may be implemented as hardware (including circuits) and/or software, depending on the application requirements.

The following terminology may be useful in understanding the present disclosure. It is to be understood that the terminology described herein is for the purpose of description and should not be regarded as limiting.

5 Cryptography – A technique of protecting information by transforming a piece of information (encrypting it) with a secret encryption key into an unintelligible format. Only users who possess the secret key may be able to decipher (or decrypt, or recover) the message into the original piece of information. Cryptography systems are broadly classified into symmetric-key systems that use a single private
10 key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that is only known to the recipient of the message.

 Encryption and decryption – Encryption is the process of transforming
15 information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again.

 Cryptographic algorithm and key – A cryptographic algorithm is a mathematical function used for encryption or decryption. In most cases, the ability
20 to keep encrypted information confidential is based not on the cryptographic algorithm, which is widely known, but on a number called a 'key' that is used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is virtually impossible. Encryption strength is often described in terms of
25 the size of the keys used to perform the encryption: in general, longer keys provide stronger protection of information.

Authentication – It is the process of confirming an identity. In the context of smart batteries, authentication involves the confident identification of a genuine smart battery by another device external to the smart battery.

5 Counterfeit smart batteries may not provide adequate safeguards to protect the occurrence of unsafe conditions such as over heating during the charging process. In some instances the over heating condition may cause an explosion. There is a need to ensure the safe and secure operation of information system device and the smart battery, especially during the charging phase of the smart
10 battery. According to one embodiment, in a method and system for authenticating a smart battery for charging, the smart battery receives an encrypted random string. In this embodiment, the device performs the encryption function and the smart battery performs the decryption function. A controller of the device generates the encrypted random string by generating a random string and encrypting the random
15 string with an encryption key. The smart battery decrypts the encrypted random string with the encryption key to recover the random string and transfer the random string to the controller. The controller verifies that the random string is unchanged to authenticate the smart battery for the charging. If the random string has been modified then the smart battery is disabled from the charging.

20 FIG. 1 illustrates a diagrammatic representation of a smart battery authentication system 100 for authenticating a smart battery 110, according to an embodiment. The smart battery 110 and/or an AC power source 140 provides power to a portable information handling system device 101. The smart battery
25 authentication system 100 includes: 1) the smart battery 110 having a smart electronics 112 and at least one rechargeable cell 116, 2) a controller 170 included in the portable device 101 for controlling the operation of power sources such as the battery 110 via control line 172 and the AC power source 140, 3) the AC power source 140, 4) an AC/DC adaptor device 130 for converting the AC voltage/power to

DC voltage/power, 5) a charger device 120 providing the charge to the smart batteries 110 via a charge line 152, 6) an AC power source switch 132 for controlling the flow of power from the AC/DC adaptor 130 to the portable device 101 by control line 164, and 7) a primary discharge switch 134 for controlling the flow of power from the smart battery 110 to the portable device 101 by control line 166, and 8) a primary charge switch 144 for controlling the flow of power from the charger 120 to the smart battery 110 by control line 162.

In one embodiment, items 1-2, and 5-8 may be included in the device 101, while items 3 and 4 are external to the device 101. In one embodiment, a power supply system (not shown) includes items 1, and 4-8. In one embodiment, the device 101 includes an electrical circuit (not shown) operable to provide a charge to the smart battery 110.

In one embodiment, each of the switches 132, 134 and 144 are implemented using MOSFET body diode devices. The MOSFET body diodes are advantageously used to minimize the impact of an accidental reverse connection of the battery 110 or other over-current causing conditions. The MOSFET body diodes are also useful to maximize the availability of power to the device 101.

The controller 170 included in the portable device 101 is operable to control various inputs and outputs of the device 101. For example, the controller 170 may be used to control inputs and outputs of a keyboard (not shown) of the device 101 via a bus (not shown) such as the SMBus (not shown). In this embodiment, the controller 170 is operable to authenticate the smart battery 110. The controller 170 advantageously safeguards the charging process by enabling authenticated smart batteries to receive the charge from the charger device 120 and disabling counterfeit smart batteries from receiving the charge. As described herein any smart battery,

which has failed the authentication process, is identified as a counterfeit smart battery.

The controller 170 is operable to receive inputs from various power sources and loads to control the flow of power from the various sources of power such as the smart battery 110 and the AC power source 140 to the various loads such as the portable device 101. The controller 170 controls the charger 120 by a control line 161. In one embodiment, a Basic Input Output System (BIOS) program (not shown) may be used to receive inputs and generate outputs.

In one embodiment, the battery charge line 152 and the control lines 162, 172, 164, 166 may be implemented using the SMBus (not shown). In one embodiment, the battery charge line 152 and the control lines 162, 172, 164, 166 may be implemented using dedicated, electrically conducting lines or paths.

The smart battery 110 includes the smart electronics 112 to control the operating condition of the battery 110 and monitor various battery variables such as voltage, current, temperature, and charge level. The smart battery 110 includes at least one rechargeable cell 116. Other cells may be present but are not shown.

The smart electronics 112 is electrically coupled to the battery charge line 152 and the control line 172 for interfacing with external devices such as the charger device 120 and the controller 170 respectively. Another embodiment of the smart battery 110 is described in FIG. 2.

The smart electronics 112 and the controller 170 jointly control: a) the operating condition of the smart battery 110 such as the charging or discharging operation, and b) the authentication process of the smart battery 110 to enable the charging operation. More specifically, the smart electronics 112 monitors the energy level of the rechargeable cell 116. When requested by the controller 170, the smart

electronics 112 is operable to provide energy stored in the rechargeable cell 116 to the portable device 101 during a discharge operating condition. The smart electronics 112 is operable to notify the controller 170 when the energy level of the rechargeable cell 105 falls below a predefined threshold level. During a charge
5 operating condition, the smart electronics 112 is operable to receive a charge from the charger 120 via the charge line 152 and transfer the charge to the rechargeable cell 116 when required.

In one embodiment, the controller 170 generating a random string initiates
10 the authentication process. Additional details of the authentication process are described in FIG. 3. The random string includes alphanumeric characters. In one embodiment, the random string is a random number. The controller 170 also includes encryption hardware or software to encrypt the random string with an encryption key. In one embodiment, the encryption key is of a predefined length
15 and is private. The output of the encryption process performed by the controller 170 is an encrypted random string. In one embodiment, a processor (not shown) of the device 101 performs the generation of the random string and the encrypted random string.

20 The smart electronics 112 of the smart battery 110 is operable to receive the encrypted random string generated by the controller 170. The smart electronics 112 decrypts the encrypted random string with the same encryption key used by the controller 170 for the encryption process. As a result of the decryption process the smart electronics 112 recovers the random string. The random string, which has
25 been recovered by the smart battery 110, is transferred to the controller 170 for authentication. The controller 170 authenticates the smart battery 110 by determining if the random string has changed compared to the original. If there is no change in the random string then the smart battery 110 is authentic. However, if

the random string has changed then the smart battery 110 is identified as a counterfeit.

FIG. 2 illustrates a diagrammatic representation of the smart battery 110 having a processor 210 and the smart electronics 112, according to an embodiment. In this embodiment, the functions associated with the authentication process are performed by the processor 210, while the smart electronics 112 is operable to control the operating condition of the battery 110 and monitor various battery variables as described earlier.

The authentication process is implemented using a single encryption step and a single decryption step described earlier in FIG. 1. In one embodiment, to further improve the authentication process a two-step encryption/decryption process is implemented, as described in further detail in FIG. 3. In the two-step authentication process the smart battery 110 performs the decryption as well as the encryption step. Thus, the processor 210 is operable to advantageously perform the encryption and/or decryption functions described earlier. In addition, the processor 210 also handles communications with the controller 170 through the control line 172, and with the smart electronics through a control line 274. In one embodiment, control lines 172 and 274 use the SMBus. The addition of the processor 210 advantageously reduces the complexity of the smart electronics 112.

FIG. 3 is a flow chart illustrating a method for authenticating the smart battery 110, according to one embodiment. In this embodiment, a two-step authentication process for authenticating the smart battery 110 is described. In step 310, the controller 170 generates a first random string. The first random string includes alphanumeric characters. In one embodiment, the first random string is a random number. In step 320, the controller 170 includes encryption hardware or software to encrypt the first random string with a first encryption key. In one embodiment, the

first encryption key is of a predefined length and is private. The output of the encryption process performed by the controller 170 is a first encrypted random string. In step 330, the controller 170 (acting as the master device) transfers the first encrypted random string to the smart battery 110 (acting as the slave device). In
5 step 340, the smart battery 110 decrypts the encrypted first random string with the first encryption key to recover a second random string. The second random string may or may not be the same as the first random string depending on the authenticity of the smart battery 110. In step 350, the smart battery 110 encrypts the second
10 random string with a second encryption key to generate the encrypted second random string. In step 360, the encrypted second random string is transferred from the smart battery 110 to the controller 170. In step 370, the controller 170 decrypts the encrypted second random string with the second encryption key to recover the second random string. In step 380, authentication of the smart battery 110 includes verifying the first random string and the second random string match. In step 390, if
15 the smart battery 110 is identified to be authentic then the charging operation is enabled. In step 395, if the smart battery 110 is identified to be a counterfeit then the charging operation is disabled.

Various steps described above may be added, omitted, combined, altered, or
20 performed in different orders. For example, steps 310, 320 and 330 may be combined into a single step 335 in which the smart battery 110 receives the encrypted first random string.

FIG. 4 illustrates a block diagram of an information handling system to
25 implement method or apparatus aspects of the present disclosure, according to an embodiment. For purposes of this disclosure, an information handling system 400 may include any instrumentality or aggregate of instrumentalities operable to compute, classify, process, transmit, receive, retrieve, originate, switch, store, display, manifest, detect, record, reproduce, handle, or utilize any form of

information, intelligence, or data for business, scientific, control, or other purposes. For example, the information handling system 400 may be a personal computer, a network storage device, or any other suitable device and may vary in size, shape, performance, functionality, and price.

5

The information handling system 400 may include random access memory (RAM), one or more processing resources such as a central processing unit (CPU) or hardware or software control logic, ROM, and/or other types of nonvolatile memory. Additional components of the information handling system may include
10 one or more disk drives, one or more network ports for communicating with external devices as well as various input and output (I/O) devices, such as a keyboard, a mouse, and a video display. The information handling system may also include one or more buses operable to transmit communications between the various hardware components.

15

Referring to FIG. 4, the information handling system 400 includes a processor 410, a system random access memory (RAM) 420, a system ROM 422, a display device 405, a keyboard 425 and various other input/output devices 440. It should be understood that the term "information handling system" is intended to encompass
20 any device having a processor that executes instructions from a memory medium. The information handling system 400 is shown to include a hard disk drive 430 connected to the processor 410 although some embodiments may not include the hard disk drive 430. The processor 410 communicates with the system components via a bus 450, which includes data, address and control lines. A communications
25 device (not shown) may also be connected to the bus 450 to enable information exchange between the system 400 and other devices.

In one embodiment, the information handling system 400 may be used to implement the portable information handling system device 101 described in FIG. 1.

The smart battery system 110 (not shown) may be configured to provide power to the information handling system 400. In one embodiment, the processor 210 and processor 410 may be similar.

5 The processor 410 is operable to execute the computing instructions and/or operations of the information handling system 400. The memory medium, e.g., RAM 420, preferably stores instructions (also known as a "software program") for implementing various embodiments of a method in accordance with the present disclosure. In various embodiments the one or more software programs are
10 implemented in various ways, including procedure-based techniques, component-based techniques, and/or object-oriented techniques, among others. Specific examples include assembler, C, XML, C++ objects, Java and Microsoft Foundation Classes (MFC). For example, in one embodiment, the BIOS program described may be implemented using an assembler language code.

15 Although illustrative embodiments have been shown and described, a wide range of modification, change and substitution is contemplated in the foregoing disclosure and in some instances, some features of the embodiments may be employed without a corresponding use of other features. Accordingly, it is
20 appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the embodiments disclosed herein.